

JAN 27 2009

Customer No. 24498  
Appln. Serial No. 10/549,407  
Resp. to OA dated August 4, 2008

Atty. Docket No. PU030084

**Amendment to the Claims**

This listing of the claims replaces all prior versions and listings of claims in the application.  
Please amend claims 1, 5, 7 and 9-27 and add new claims 28-31 as follows:

Claim 1 (Currently amended). A method for enabling a client terminal to access a wireless network, comprising:

- receiving an access request from the client terminal;
- redirecting the access request to a local web server via a packet traffic filter for filtering packet traffic;
- requesting from the client terminal, information-required to establish client terminal access to the wireless network;
- activating, in response to the client terminal access information received from the client terminal, a module that reconfigures the client terminal for authentication using appropriate parameters associated with a configuration arrangement selected by a user; and
- authenticating the reconfigured client terminal and allowing access to the wireless network in response to the authentication.

Claim 2 (Previously presented). The method according to claim 1, wherein the wireless network is an IEEE 802.11 compliant wireless local area network (WLAN), and the client terminal is an IEEE 802.1x compliant client terminal.

Claim 3 (Previously presented). The method according to claim 2, wherein the activating step comprises activating an Active X control/plugin installed on the client terminal.

Claim 4 (Original). The method according to claim 2, wherein the activating step comprises downloading to, and activating in, the client terminal an Active X control/plugin.

Claim 5 (Currently amended). An access point for providing a secure communications session between a client terminal and a wireless network, comprising:  
means for receiving an access request from the client terminal;

Customer No. 24498  
Appln. Serial No. 10/549,407  
Resp. to OA dated August 4, 2008

Atty. Docket No. PU030084

means for redirecting the access request to a local web server for allowing a reconfigured access to the wireless network via a packet filter means for filtering packet traffic,

means for requesting from the client terminal, information to establish client terminal access to the wireless network;

means for activating, in response to the client terminal access information received ~~from~~ from the client terminal, a software module that reconfigures the client terminal for authentication using appropriate parameters associated with a configuration arrangement selected by a user; and

means for authenticating the reconfigured client terminal and allowing access to the wireless network in response to the authentication.

Claim 6 (Original). The access point according to claim 5, wherein the access point complies with the IEEE 802.11 standards and the client terminal is an IEEE 802.1x compliant client terminal.

Claim 7 (Currently amended). A method for configuring a client terminal to provide secure access in a wireless network, comprising:

filtering traffic associated with a ~~first~~ request from the client terminal for access to the wireless network, at a packet traffic filter for filtering packet traffic;

redirecting the access request to a designated web server, via said packet traffic filter for filtering packet traffic; and

issuing a provider list web page and a ~~second~~ request from the designated web server to the client terminal for provider selection information ~~required~~ to establish an authorized communication.

Claim 8 (Previously presented). The method according to claim 7, wherein the wireless network is an IEEE 802.11 compliant wireless local area network and the client terminal is an IEEE 802.1x compliant client terminal.

Claim 9 (Currently amended). The method according to claim 7, further comprising the

Customer No. 24498  
Appln. Serial No. 10/549,407  
Resp. to OA dated August 4, 2008

Atty. Docket No. PU030084

~~designated web server~~ receiving from the client terminal ~~and communicating to the designated web server~~ said provider selection information required to establish for establishing an said authorized ~~connection~~ communication.

Claim 10 (Currently amended). The method according to claim ~~79~~, further comprising the client terminal receiving information corresponding to parameters from the designated web server and ~~communicating to the client terminal~~ including access transmission rate information required to for establishing establish an said authorized communication.

Claim 11 (Currently amended). The method according to claim ~~9~~, further comprising the client terminal receiving information corresponding to parameters from the designated web server ~~including and communicating to the client terminal~~ access user account creation information for establishing required to establish an said authorized communication.

Claim 12 (Currently amended). The method according to claim ~~79~~, further comprising the client terminal receiving information corresponding to parameters from the designated web server and ~~communicating to the client terminal~~ access including authentication method selection information required to establish for establishing an said authorized communication.

Claim 13 (Currently amended). The method according to claim ~~79~~, further comprising the client terminal receiving information corresponding to parameters from the designated web server and ~~comprising communicating to the client terminal~~ including new account creation information procedures required to establish for establishing an said authorized communication.

Claim 14 (Currently amended). The method according to claim ~~79~~, further comprising the client terminal receiving information corresponding to parameters from the designated web server and ~~communicating to the client terminal~~ including access user terms and conditions of acceptance information required to establish for establishing an said authorized communication.

Claim 15 (Currently amended). The method according to claim ~~710~~, further comprising

Customer No. 24498  
Appln. Serial No. 10/549,407  
Resp. to OA dated August 4, 2008

Atty. Docket No. PU030084

~~receiving from the client terminal and communicating to the designated web server access rate information required to establish~~ for establishing ~~ansaid~~ authorized communication.

Claim 16 (Currently amended). The method according to claim ~~711~~, further comprising ~~receiving from the client terminal and communicating to the designated web server user account creation data required to establish~~ information to the designation web server for establishing ~~ansaid~~ authorized communication.

Claim 17 (Currently amended). The method according to claim ~~712~~, further comprising ~~receiving from the client terminal and communicating to the designated web server user access authentication method selection information to the designated web server required to establish~~ for establishing ~~ansaid~~ authorized communication.

Claim 18 (Currently amended). The method according to claim ~~714~~, further comprising ~~receiving from the client terminal and communicating to the designated web server acceptance of the user access terms and conditions of acceptance information for establishing required to establish an~~ said authorized communication.

Claim 19 (Currently amended). The method according to claim ~~89~~, whereby ~~authorization~~ authentication is browser based and related to said provider list web page and the method further comprising invoking the browser program is an ActiveX control to reconfigure the client terminal.

Claim 20 (Currently amended). The method according to claim 8, whereby authentication is browser based and the method further comprising sending an ActiveX control to configure the client terminal. a software module of said client terminal reconfiguring the client terminal and establishing said authorized communication ~~the browser program is a plug-in.~~

Claim 21 (Currently amended). A mobile terminal, comprising:

Customer No. 24498  
 Appl. Serial No. 10/549,407  
 Resp. to OA dated August 4, 2008

Atty. Docket No. PU030084

means for receiving an extended authentication protocol request identification message packet;

means for forwarding an extended authentication protocol response identity message packet;

means for receiving an extended authentication protocol failure message packet;

means for forwarding a web ~~re-direct~~access request via a packet traffic filter for filtering packet traffic as a web request redirect message;

means for receiving a provider list web page;

means for selecting a provider and means for forwarding said-selected provider information to a designated web server;

means for receiving an ActiveX control/plug-in message from the designated web server to re-configure/reconfigure said mobile terminal; and

means for reconfiguring said mobile terminal and establishing authorized communications.

Claim 22 (Currently amended). The~~A~~ method as recited in claim 1, the method further comprising

creating a plurality of ~~operating~~operational states including a progress state and a failure state, said packet traffic filter receiving wireless local area network failure state information via a redirected client message and moves a reconfiguration process to said local web server via a web request redirect message~~from said access point~~.

Claim 23 (Currently amended). The~~An~~ access point as recited in claim 5, the access point creating a plurality of ~~operating~~operational states including a progress state and a failure states wherein said packet traffic filter means receives wireless local area network failure state information via a redirected client message and moves a reconfiguration process to said local web server via a web redirect message ~~from said access point~~.

Claim 24 (Currently amended). An access point associated with a communications network, comprising:

Customer No. 24498  
 Appln. Serial No. 10/549,407  
 Resp. to OA dated August 4, 2008

Atty. Docket No. PU030084

means for forwarding an extended authentication protocol request identification message packet to a client terminal;

means for receiving an extended authentication protocol response identity message packet from the client terminal;

means for forwarding an extended authentication protocol failure message packet to a client terminal responsive to a state failure;

means for receiving a re-direct client request from said forwarding means at a packet filter module responsive to said state failure;

alternative means for receiving a request for access to a communications network at said packet filter module responsive to said state failure; and

means for forwarding a web ~~re-direct~~ request redirect via ~~from~~ said packet filter module to a designated web server and for establishing authorized communications following receipt of selected provider information at the designated web server and successful client terminal reconfiguration responsive to authentication.

Claim 25 (Currently amended). The method according to claim 1, further comprising:

detecting a state failure responsive to receipt of an EAP response identity packet and to receipt of a RADIUS access request reject message; and

redirecting the access request to a local web server via said packet traffic filter responsive to one of the packet traffic filter receiving a redirect client request and of receiving a web access request from said client terminal after detection of said state failure.

Claim 26 (Currently amended). The access point according to claim ~~five~~5, further comprising:

an IEEE 802.1x engine for converting the access request to a RADIUS message, for responding to a RADIUS access reject message and for detecting a state failure; and

said packet traffic filter means redirecting the access request to a local web server responsive to one of the packet traffic filter means receiving a redirect client request from said IEEE 802.1x engine and of receiving a web access request from said client terminal after the IEEE 802.1x engine ~~detection of~~ detecting said state failure.

Customer No. 24498  
Appln. Serial No. 10/549,407  
Resp. to OA dated August 4, 2008

Atty. Docket No. PU030084

Claim 27 (Currently amended). The method according to claim 7, further comprising:  
detecting a state failure responsive to receipt of an EAP response identity packet and to receipt of a RADIUS access request reject message; and  
redirecting the access request to said designated web server via said packet traffic filter responsive to one of the packet traffic filter receiving a redirect client request and of receiving a web access request from said client terminal after detection of said state failure.

Claim 28 (New). The method according to claim 1 wherein said information to establish client terminal access to the wireless network comprises provider selection information responsive to receipt of a provider list web page at the client terminal from said local web server.

Claim 29 (New). The access point according to claim 5 wherein said information to establish client terminal access to the wireless network comprises provider selection information responsive to receipt of a provider list web page at the client terminal from said local web server.

Claim 30 (New). The mobile terminal according to claim 21 wherein said provider list web page and said ActiveX control/plugin are received from a local web server in response to receipt of a web request redirect message from an access point.

Claim 31 (New). The access point according to claim 24 wherein said designated web server transmits an ActiveX control/plugin for configuring the client terminal responsive to the receipt of selected provider information at the designated web server.